

WHAT IS CLAIMED IS:

Sub A1
1. In an operating system on a computing system wherein requests are in the form of encapsulated information, a method for controlling access to actions and objects within the computing system, said computing system providing facilities for the instantiation of said objects and performance of said actions, said method comprising:

configuring selected domains on said computing system as configured domains, each one of said configured domains comprising a higher-order multidimensional domain space, for segregating system operational functionality according to defined operational boundaries, said operational boundaries defined by mapping attributes of the requests into individual domains;

providing a master daemon, said master daemon selecting said configured domains by utilizing said attributes of the requests;

causing said master daemon to respond to selected ones of said requests to perform at least one of the following actions on said computing system:

instantiating on said operating system at least one subordinate daemon;

instantiating on said operating system at least one subordinate process;

instantiating on said operating system at least one subordinate thread;

performing at least one other defined action;

wherein said subordinate daemons, said subordinate processes, said subordinate threads, and said other defined actions being constrained to operate within one of said configured domains at least as restrictive as the configured domain of said master daemon.

2. The method according to claim 1, wherein said master daemon is further operative to:

009090" T0999560

control functionality of all said instantiated subordinate daemons, subordinate processes, subordinate threads and said defined actions on said operating system in said computer system.

3. In an operating system on a computing system according to claim 1, wherein said master daemon is further operative to:

interface with said computing system to maintain centralized and coordinated access to auditing subsystems of said operating system.

4. The method according to claims 1-3 wherein said selected domains are further defined by at least one of a security label, a set of security labels, a lattice of security labels, a group of security labels, a range of security labels, a combination of collections of security labels, and other defined constructs.

5. In an operating system on a computing system connected to a network of computing systems wherein requests are in the form of encapsulated information, a method for controlling access to actions and objects within any of the computing systems, said computing systems providing facilities for the remote instantiation of said objects and performance of said actions, said method comprising:

configuring selected domains on at least one of said computing systems as configured domains, each one of said configured domains comprising a higher-order multidimensional domain space for segregating system operational functionality according to defined operational boundaries, said operational boundaries defined by mapping attributes of the requests into individual operating domains;

providing a master daemon, said master daemon selecting said configured domains by utilizing said attributes of the requests;

causing said master daemon to respond to selected ones of said requests to perform at least one of the following actions on at least one of said computing systems:

instantiating at least one daemon;

instantiating at least one subordinate daemon;

instantiating at least one process;

18 instantiating at least one subordinate process;
19 instantiating at least one subordinate thread;
20 performing at least one other defined action;
21 wherein said daemons, said subordinate daemons, said
22 processes, said subordinate processes, said subordinate threads, and said
23 other defined actions being constrained to operate within one of said
24 configured domains at least as restrictive as the configured domain of said
25 master daemon.

1 6. The method according to claim 5 wherein at least one of said
2 computing systems is local to said master daemon.

1 7. The method according to claim 6 wherein at least one of said
2 computing systems is on said network and is remote from said master daemon.

1 8. The method according to claim 5 wherein at least one of said
2 computing systems is on said network and is remote from said master daemon.

1 9. The method according to claim 8 further including the step of:
2 causing said master daemon to respond to selected ones of said requests to
3 perform a defined action on said remote computing system.

1 10. The method according to claim 9, wherein said master daemon is
2 further operative to:

3 control functionality of all said instantiated daemons, subordinate
4 daemons, processes, subordinate processes, subordinate threads and said defined actions
5 on selected ones of said operating systems on computer systems connected to said
6 network.

1 11. In an operating system on a computing system connected to a
2 network of computing systems according to claim 10, wherein said master daemon is
3 further operative to:

4 interface with said local computing system and said remote computing
5 systems to maintain centralized and coordinated access to auditing subsystems of said
6 computing systems connected to said network of computing systems.

1 12. The method according to claims 5-11 wherein said selected
2 domains are further defined by at least one of a security label, a set of security labels, a
3 lattice of security labels, a group of security labels, a range of security labels, a
4 combination of collections of security labels, and other defined constructs.

09588801.050600